We claim:

1. An apparatus for verifying the security integrity of remote network devices, comprising:

a proxy device for receiving a request for network services by at least one remote network device and performing a security integrity scanning operation on the requesting remote network device; and

an authorization processing unit and access control rules unit for determining if the remote network device is authorized to access the requested network services based on the results of the security scanning operation.

2. The apparatus as recited in claim 1, wherein the proxy device makes integrity security decisions regarding access to network services by a remote network device on a request-by-request basis.

3. The apparatus as recited in claim 1, wherein the access control rules unit includes a plurality of variables used to generate a set of security properties for each remote network device.

4. The apparatus as recited in claim 3, wherein the set of security properties may be different for each remote network device that accesses and requests service through the network.

5. The apparatus as recited in claim 1, wherein the proxy device uses at least one script to select of the type of scanning operations to be performed for each remote network device accessing the network.

6. The apparatus as recited in claim 5, wherein the proxy device uses a Java applet for executing the desired script on the remote network device.

7. The apparatus as recited in claim 6, wherein a signed applet, executing the script, is allowed to access the remote network device for the purposes of executing programs as well as searching and reading specific data files that reside on the remote network device.

8. The apparatus as recited in claim 1, wherein the authorization processor refers to a series of variable values in the access control rule unit to determine if a remote network device is authorized to access the requested network service.

9. A system for verifying security integrity of remote network devices, comprising:

at least one remote network device that accesses a network via a network connection to make a request for one or more network resident services;

a gateway device for receiving the request for services and performing a security integrity scanning operation on the remote network device prior to allowing access to the requested network services;

an authentication server that verifies user authentication credentials of users of remote network devices that access the network; and

at least one network server that provides requested network services to at least one remote network device accessing the network through the gateway device.

10. The system as recited in claim 9, wherein the gateway device further comprises a proxy server for establishing a data communication connection between the remote network device and the network server.

11. The system as recited in claim 9, wherein said gateway device further comprises an access control rules unit used to determine if a remote network device is authorized to access the requested network services.

12. The system as recited in claim 9, wherein the gateway device makes integrity security decisions regarding access to network services by a remote network device on a request-by-request basis.

13. The system as recited in claim 9, wherein the access control rules unit includes the plurality of variables used to generate a set of security properties for each remote network device.

14. The system as recited in claim 13, wherein the set of security properties may be different for each remote network device that accesses and requests service through the network.

15. The system as recited in claim 9, wherein the proxy device uses at least one script to select of the type of scanning operation to be performed for each remote network device accessing the network.

16. The system as recited in claim 15, wherein the proxy device uses a Java applet for executing the desired script on the remote network device.

17. The system as recited in claim 16, wherein a signed applet, executing the script, is allowed to access the remote network device for the purposes of executing programs as well as searching and reading specific data files that reside on the remote network device.

18. The system as recited in claim 9, further comprising the use of SSL to protect data communicated between the remote device and the gateway device.

19. The system as recited in claim 11, wherein the gateway device further comprises an authorization processor that refers to a series of variable values in the access control rule unit to determine if a remote network device is authorized to access the requested network service.

20. The system as recited in claim 9, wherein the networks used for establishing communication between said remote device and said gateway uses GSM, GPRS, WAP, EDGE, UMTS or other similar wireless network protocol.

21. The system as recited in claim 9, wherein the remote network device can either be a public kiosk, personal computer, cellular telephone, satellite telephone, personal assistant or Bluetooth device.

22. A method for verifying security integrity of remote network devices, that includes the steps of:

defining at least one variable used as a vehicle to convey the results of the scanning process;;

downloading verification software via a network connection to the remote network device that performs scanning process and reports result used in scanning script. includes at least one variable

performing at least one scanning operation on the remote network device to verify the security integrity of the remote device; and

obtaining the results of the scanning operation for purposes of determining whether or not the remote network device is authorized to access the requested network services.

23. The method as recited in claim 22 wherein, the making of security decisions with regard to a request for network services by a remote network device is done on a per-request basis.

24. The method as recited in claim 22 wherein, an array of variables to used to generate a set of security properties for each remote network device.

25. The method as recited in claim 24, wherein the set of security properties may be different for each remote network device that accesses and requests service through the network.

26. The method as recited in claim 22, also includes selecting s at least one script for the type of scanning operation to be performed for each remote network device that accesses the network.

27. The method as recited in claim 26, also includes executing the desired script on the remote network device is done by using a signed Java applet.

28. The method as recited in claim 16, wherein using a signed applet executing the script to access the remote network device for the purposes of executing programs as well as searching and reading specific data files that reside on the remote network device.

29. The method as recited in claim 22, wherein assigning a values to a set of variables in the verification software resulting from the scanning process of the remote network device.

30. The method as recited in claim 22, wherein using SSL to protect the data communicated between the remote device and the gateway.

31. The method as recited in claim 29, wherein referencing to an assigned series of variable values in the access control rules determines if a remote network device is authorized to access the requested network service.

32. The method as recited in claim 22, wherein making authorization decisions based in part on results returned by the scanning process.

33. The method as recited in claim 22, wherein transmitting and receiving data, information and applications content between a remote device and the gateway using either GSM, GPRS, WAP, EDGE, UMTS or other similar wireless network protocol.

34. The method as recited in claim 22, wherein the remote network device is a public kiosk, personal computer, cellular telephone, satellite telephone, personal assistant or Bluetooth device.

35. A method for assessing the integrity of remote network devices for purposes of regulating access to network services via a network gateway comprising the steps of:

defining at least one access control policy for accessing network services wherein the access control policy depends, at least in part, on the results of an integrity scan performed on the remote network device;

downloading verification software that an administyrator can specify what scan scripts are to used under what conditions to the remote network device;

performing an integrity scan on the remote network device and conveying at least one result of the scan to a gateway device; and

regulating access by the remote network device to network services via the gateway device based, at least in part, on the results of the integrity scan.

36. The method as recited in claim 35, wherein making access control decisions with regard to a remote network device on a per-service basis.

37. The method as recited in claim 35, wherein using at least one defined variable in each access control policy.

38. The method as recited in claim 35, wherein sending the results of the integrity scan to the gateway in the form of an assigned value for the defined variable.

39. The method as recited in claim 35 wherein using a script to specify the integrity scan operations that will be performed on the remote network device.

40. The method as recited in claim 35, wherein using a signed Java applet as the verification software to be downloaded to the remote network device.

41. The method as recited in claim 39, wherein using a signed applet executing the script to access the remote network device for the purposes of executing programs as well as searching and reading specific data files that reside on the remote network device.

42. The method of claim 35, wherein a plurality of variables is used to determine the access control policy for each remote network device accessing the network.

43. The method as recited in claim 42, wherein the access control policy for each remote network device is different.

44. The method as recited in claim 38, wherein referencing to an assigned series of variable values in the access control rules determines if a remote network device is authorized to access the requested network service.

45. The method as recited in claim 35, wherein using SSL to protect data communicated between the remote device and the gateway.

46. The method as recited in claim 35, wherein making authorization decisions based in part on results returned by the scanning process.

47. The method as recited in claim 35, wherein transmitting and receiving data, information and applications content between a remote device and the gateway using either GSM, GPRS, WAP, EDGE, UMTS or other similar wireless network protocol.

48. The method as recited in claim 35, wherein the remote network device is a public kiosk, personal computer, cellular telephone, satellite telephone, personal assistant or Bluetooth device.